Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Криптографія»

Лабораторна робота №2.
Криптоаналіз шифру Віженера

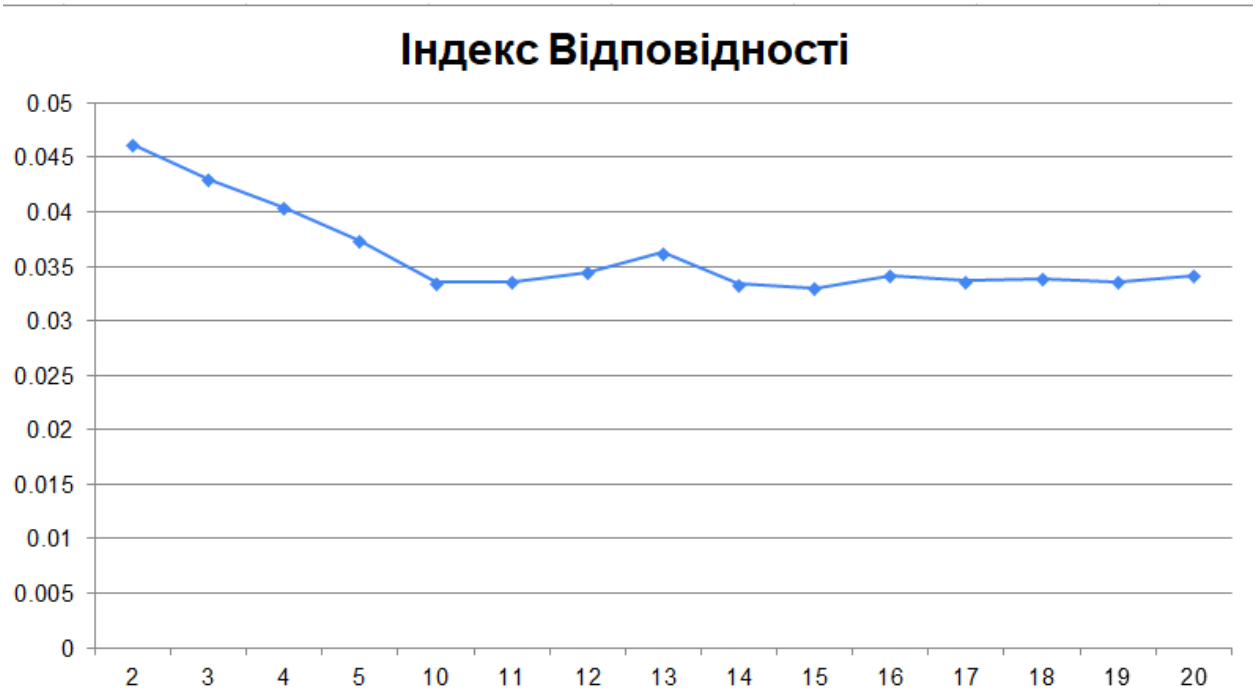
Виконали
:
студенти гр. ФБ-92
Кудряшов М.О. та Курганський Л. С.

Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Завдання 1-2
Підібраний текст для шифрування - Текст з першої лабороторної.

Таблиця ключів довжини 2-5, 10-20 та їх індекс відповідності

Довжина Ключа	Ключ	Індекс відповідності
2	йц	0.04624830630077107
3	уке	0.04296082677466156
4	нгшщ	0.040412764598953516
5	зхфыи	0.03740409560827775
10	вапролджєя	0.0335363499530644
11	чсмитьбюфывап	0.033628055357101325
12	йфяцычувскам	0.03448841459015417
13	ипенртьогшлбщ	0.03626592282423914
14	йцукенрпавыфяч	0.033391655006262504
15	ячсмитьбюфывапр	0.03301096032935611
16	йысаертьлщшгроне	0.034232879807025225
17	йфывмсапрнкеготри	0.03367107907058732
18	йцывукаепрнроггшол	0.033866794786837344
19	лшгнепротимсакувчыц	0.033632426750450174
20	ячспролдбьтименпакет	0.034156188695641986



Завдавння 3

Після того як ми отримали блоки з інформацією різних довжин, підрахували індекс схожості (індекс відповідності - математичне очікування) щоб знайти довжину ключа.

Довжина Ключа	Індекс схожості	Довжина Ключа	Індекс схожості
2	0.01596726846833301	17	0.017633782934512662
3	0.017717313069665577	18	0.01611816024792085
4	0.01328570537304865	19	0.01785401471732924
5	0.01764728575208825	20	0.01339377274247943
6	0.016038072659616535	21	0.01812483156745944
7	0.0178711435878781	22	0.016313901252191128
8	0.00820265936936896	23	0.017928019010468803
9	0.017657372554602056	24	0.008378927999161706
10	0.016019217293908317	25	0.01789058401496746
11	0.01805730403185247	26	0.015912012629175465

12	**0.013346905711734157**	**27**	**0.01797200247804008**
13	**0.017623722307630672**	**28**	**0.01355699839967598**
14	**0.016049284407321222**	**29**	**0.017648855355307892**
15	**0.017760804027040444**	**30**	**0.016318849610504137**
16	**0.0021893456544916784**	**31**	**0.017971130810908974**

Найменше значення у блоків з довжиною 16. Отримавши блоки з цією довжиною, знаходимо ключ завдяки частотному аналізу кожного з блоків. Отримали ключ “декелисоборойдей”. Дешифрувавши цей текст з цим ключем, я зрозумів що 3, 4, 13, 14 букви не вірні.
Перші 16 символів тексту - пооитноеделоулту. Можна зрозуміти, що перше слово - “понятное”, з цього розрахуємо 3 та 4 букву у ключі. Маємо “делосиоборойдей”. Далі Розшифровуємо текст з цим ключем та аналогічним способом знаходимо 13 та 14 вірні букви, отже наш ключ це “ДелоЛисОборотней”. Розшифровуємо текст повністю:

понятноеделокультурунасильновчеловеканеваоткнешьвордусиэтудовольногрустнуюистинузналинаверноелучшечемгдебытонибыловмиреКультурностьпреждевсегоусилиеиежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутунынотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпери

ивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткак
импричинамтакинесталоинтереснымничтоглавноенисветозарныевысо
тыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийис
тинноеискусствониголовокружительныебезднынакраюкоихвечнопребы
ваетнастилающаянаднимиобщепроходимыегатинауканихотябычистое
просторноесостоятельноеидобродетельноежитьестольестественноед
лябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбы
ливосновномварварамииневобычномпониманииэтогословаисстариоб
означавшеголюдейинойнеордусскойкультурыаскореевтомегозначении
котороестольжедавносделалосьобычнымвевропелюдипочтичуждыевс
якойкультурыневедающиеритуаловивозвышенныхзабототсутствиепод
линнойвоспитанностибросаетсяздесьвглазадаженевнимательномунаб
людателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшел
ковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизне
стибранноесловоиливысморкатьсяприлюднопрямовземлюпослечегос
покойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличе
ловекповзрослелизаматерелвтакомсостоянииидушиизменитьегокакпра
вилоуженельзяразвечтомудроенебовразумиттакилиначесмотряповер
оисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасил
иеневместноаувещеваниезапоздалокакимбыниуродилсяинисталчелов
екнадодатьемупрожитьжизньтаккаконхочетконечноеслионпритомневр
едитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправило
оказывалсяздесьлишьпослужебнойнадобностиводкаксегоднянесмотря
напротивныйнавевающийхандрудождикбагбылисполненлегкогопьяня
щегоазартавсегдасопутствовавшегоблизкомуиудачномузавершениюоч
ередногоделакконцуподходилорасследованиеоцелойсетичетырезавед
енияединовременноподпольныхопиумокуриленвыявленныхвразудало
мпоселкецифрыманилипрасадвернулсявалександриювдохновленный
открывшимисяперспективамивразудаломпоселкеонужевладелнесколь
кимихарчевнямиилавкамииесликприбылямотторговлиспиртныминапи
ткамиудастсядобавитьещеидоходыотопиумокурениятоможнобудетпод
уматьорасширениипредпринимательстваоприобретениииновойнедвиж
имостиииншаллабытьможетдажеобустановлениииконтролянадвсемиха
рчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащи
хлагашузаведенияхнемногочисленныеноверныеегослужителиоборудо
валиспециальныезакутыгдекуслугамжителейигостейхутуноввыстроил
исьудобныележанкиикурительныеприборыпрасадпредлагалпосетител
ямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбудней
посетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвм
ечтахужвозомнивсебякняземоразудалогоонзахотелмногоисразунанявсе

бевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиустреми
лсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниемунепринад
лежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправе
дливополагаллагашобращатьсяквэйбинамдлярешениявозникающихр
азногласийбылоневхарактереобитателейхутуновинечестныйпрасадбе
ззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьсл
агашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилс
якстычкамиоттогооказалсясильнееокончательнораспоясавшисьонсня
лсостеныдвуствольноеружьедедаиприлюднопрямопосредипереулкаот
пилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидаже
прозвищеполучилобрезагаместныежителирастерялисьопиумокурильн
ирасцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбар
ышиновеликийучительвдвадцатьвторойглавебеседисужденийнезряск
азалянезнаюниодногоправлениякотороебылобыбесконечнымисамово
льноприсвоенныйпрасадомнебесныймандатместногозначенияужеупл
ылизегорукхотялагашещеинеподозревалобэтомвскоренесколькочелов
екпотерялитрудоспособностьинтерескжизниисамоездоровьевследств
иечрезмерногоупотребленияопиуманасонгрядущийавандевятыйпопал
вбольницуулусноеведомствонародногоздоровьявсестороннеизучилоп
ричинузаболеванияванаивскореобрезагасамтогоневедаяпопалвполез
ренияуправлениявнешнейохранызаседмицустараниямибагаивзятогои
мвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэто
трозовощекийислегкаещеподетскинаивныймолодецпостепеннопревра
щаетсявсведущегоипытливогомастерасыскногоделарасположениевсе
хзаведенийгдекурилиопиумбылоопределеноснаивозможнойточностью
такжебылисоставленыподробныеспискивсехподданныхимевшихотно
шениекраспространениюопасногодляздоровьяпорокауправлениевнеш
нейохранысословочевидцевсоставилочленосборныйпортретчеловека
которыйповсемвероятиямявлялсястаршимзаправилойитакчеловекона
рушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшис
ьвгражданскоеплатьезатроесутокнепрестанногослужебногобденияуст
ановилигдеобрезагабываетпосвоимпротивуправнымделаминынчевече
ромпристечениизначительныхсилуправленияодурманиваниеордусски
хподданныхопиумомрешенобылопресечьпоусловленномусигналувэйб
инынакрываютвсенехорошиезаведенияабагсяковомчжаномзадержива
ютзаправилуиегоближниковкакталоизвестновечерниечасыпослеобхо
дасвоихвладенийивзиманияежедневнойнеправеднойданилагашсосво
имиближникамикороталвнесообразномвеселиивхарчевнекунисыновья
багещеразвзглянулначасыираздавилокуроквбронзовойпепельницепор
аонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясомм

ечномечанебылонапривычномместеродовойклинокбагаканулвнебыти
ерастворенныйядовитойслюнойзлоумногоподданногокозюлькинаэтис
обытияописаныделеополкуигоревеановыймечпрославленныйханбал
ыкскиймастерганьцзянмошуобещалотковатьлишьчерезполторагодаба
гвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножипо
дхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсея
лсясквозьгустеющиесумеркибесконечныйдождьпора

Висновок: В цій лабораторній роботі ми засвоїли методи частотного криптоаналізу та здобули навичоки роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.